



HRVATSKA
REVIZORSKA
KOMORA

Stručno savjetovanje ovlaštenih revizora u organizaciji Hrvatske revizorske komore

za 2026. godinu



HRVATSKA
REVIZORSKA
KOMORA

Provjera kibernetičke sigurnosti u reviziji

Marko Žalac

Napomena

Sadržaj ovog prezentacijskog materijala je informativnog karaktera. Upotreba prezentacijskog materijala ne oslobađa korisnika od poduzimanja potrebnih mjera predostrožnosti prije njegove uporabe, odnosno ne oslobađa korisnika od obveze primjene izvornih zakonskih odredbi i pravila struke, s toga se Hrvatska revizorska komora i autor prezentacijskog materijala ne mogu smatrati odgovornima prilikom uporabe ili u vezi s uporabom sadržaja koji se nalazi u prezentacijskom materijalu.

Uporaba sadržaja i podataka iz ovog prezentacijskog materijala dopuštena je pod uvjetom navođenja izvora podataka, osim u slučajevima kada je naznačeno drugačije.

Sadržaj

1. Kibernetički rizici iz perspektive revizije
2. MRevS 315 (izmijenjen 2019.) – IT okruženje i procjena rizika
3. Informacijska sigurnost – ključne kontrole i područja provjere
4. NIS2 – regulatorni zahtjevi i revizorski pristup
5. Zaključak

Kibernetički rizici iz perspektive revizije

Zašto je kibernetička sigurnost tema za reviziju?

- Kibernetički incidenti mogu utjecati na poslovanje i financijsko izvještavanje
- Ovisnost financijskih procesa o IT sustavima
- Rizik neovlaštenih izmjena, gubitka ili nedostupnosti podataka
- Sve veći regulatorni zahtjevi

Kibernetički rizik nije samo IT rizik – može postati rizik za financijsko izvještavanje.

Primjeri:

Ransomware

Krađa korisničkih podataka

Kompromitacija privilegiranog računa

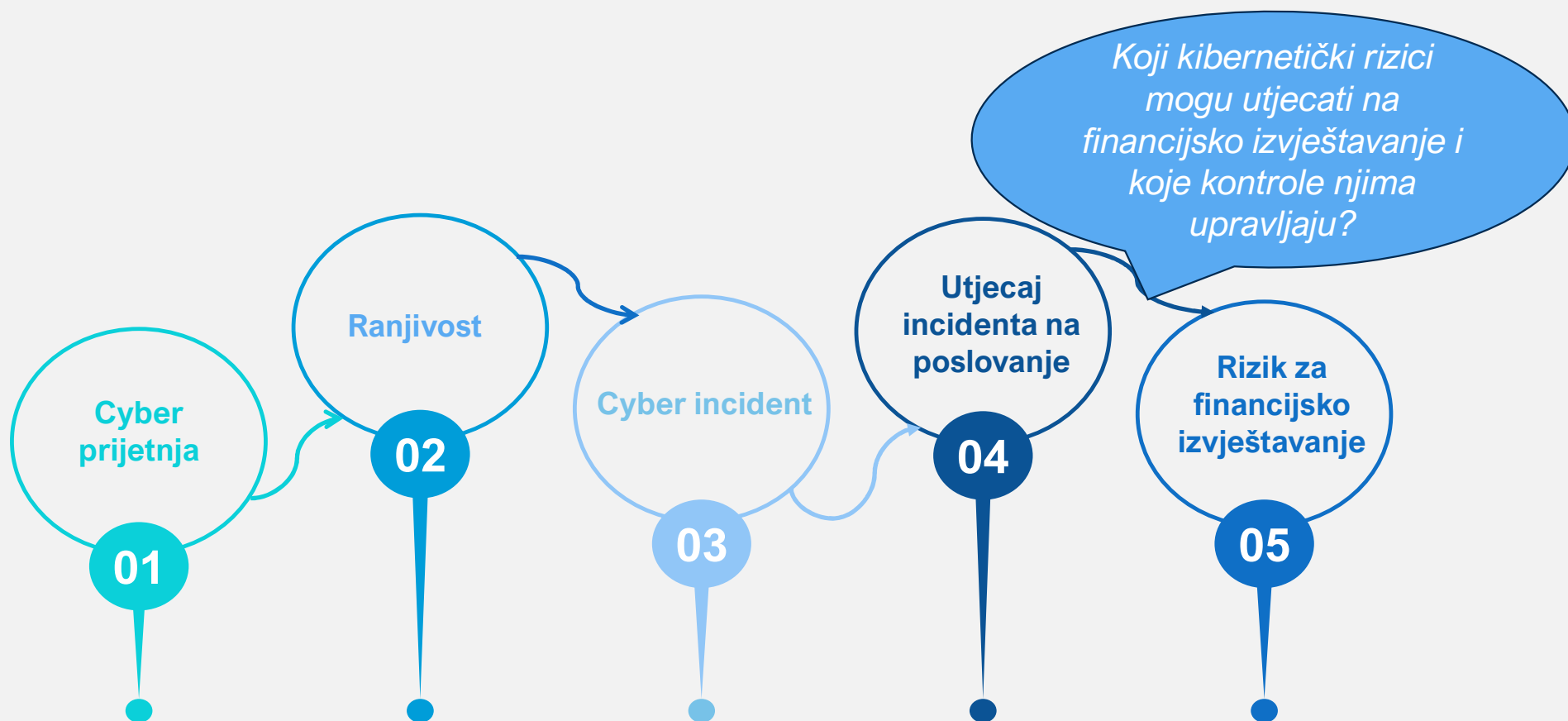
Neovlaštena izmjena podataka

Nedostupnost ključnih sustava

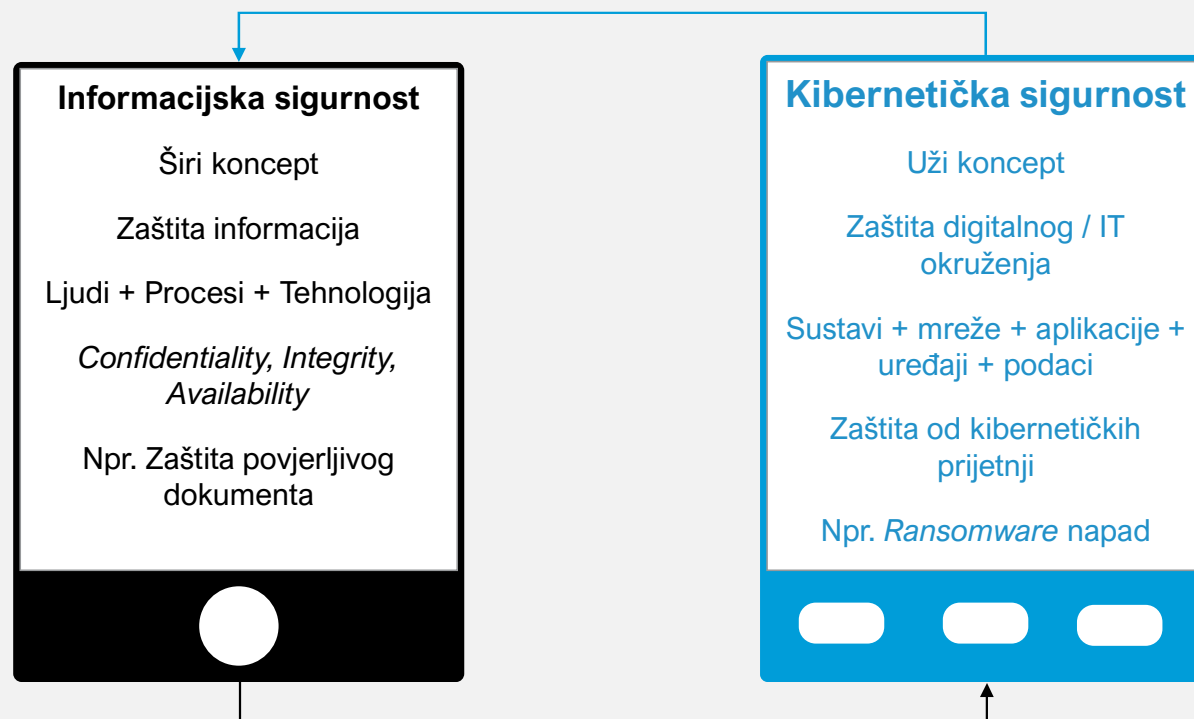
Kompromitacija dobavljača



Od kibernetičkog rizika do revizorskog rizika



Informacijska sigurnost vs. Kibernetička sigurnost



Kibernetička sigurnost je važan dio informacijske sigurnosti, ali pojmovi nisu sinonimi.

Što zapravo želimo provjeriti?



Znamo li koji su cyber rizici?



Jesu li ključni sustavi i podaci zaštićeni?



Možemo li prepoznati napad?



Možemo li učinkovito reagirati?

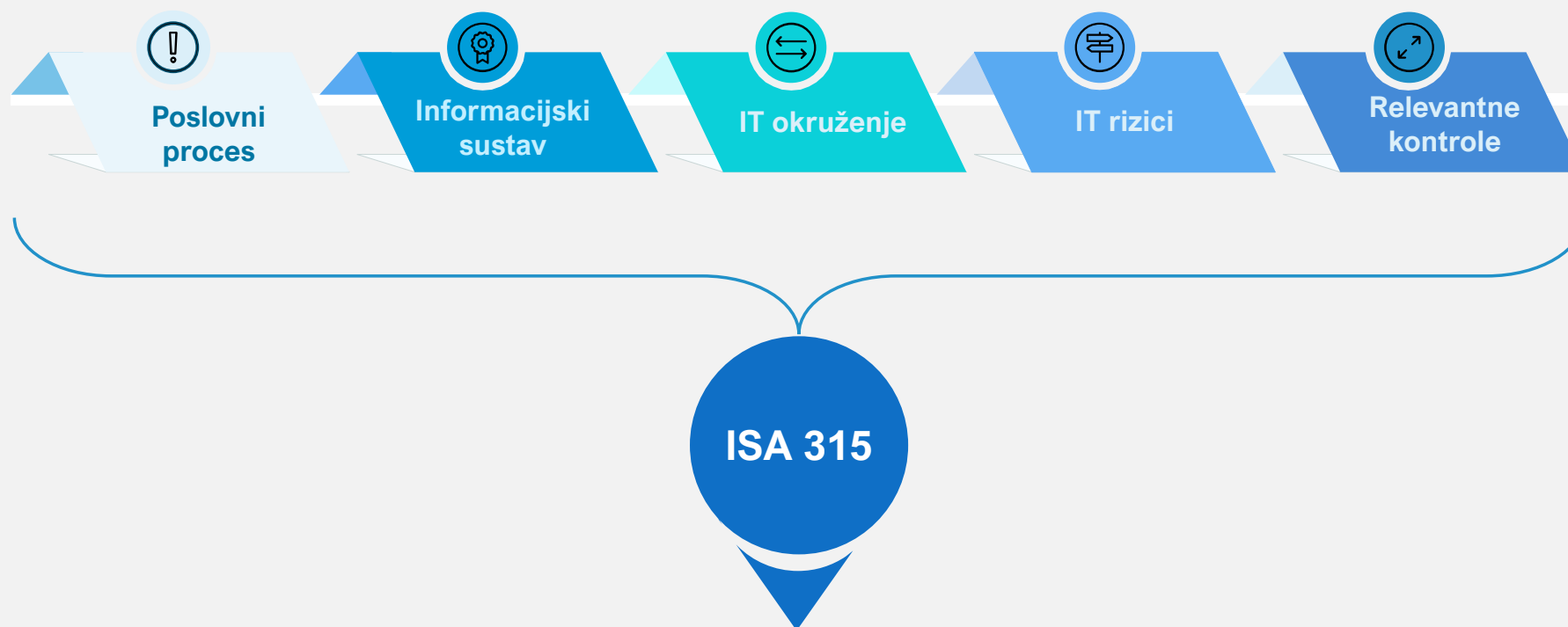


Možemo li obnoviti poslovanje?

MRevS 315 (izmijenjen 2019.)

– IT okruženje i procjena rizika

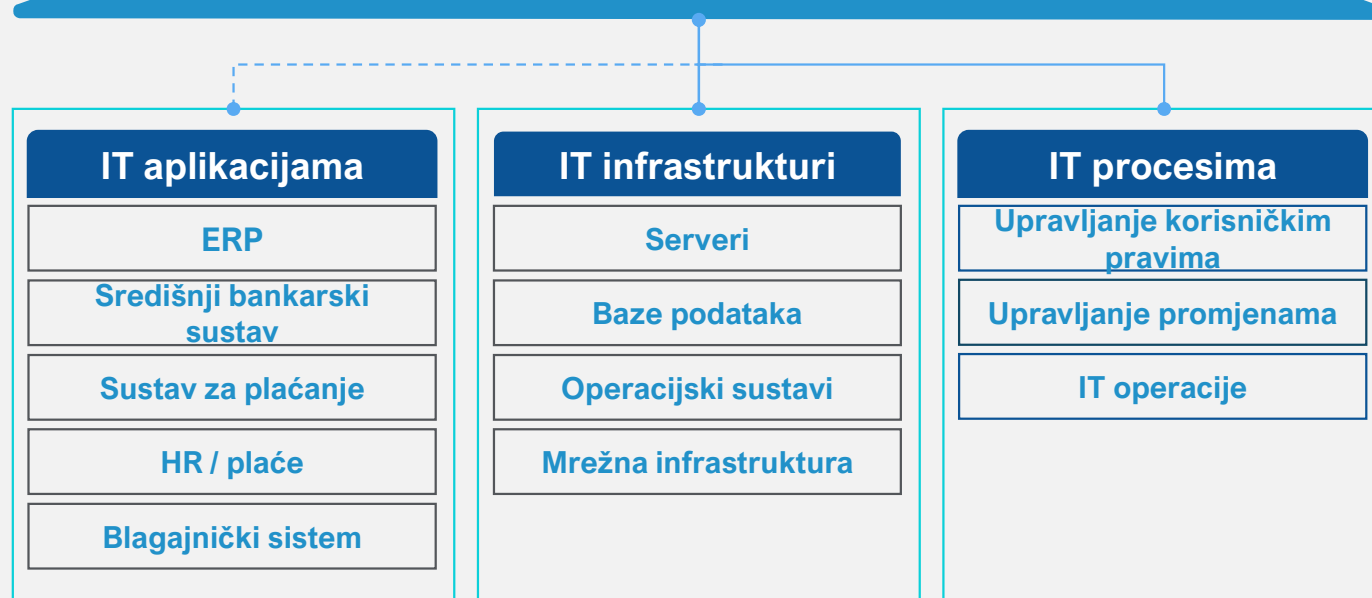
MRevS 315 (izmijenjen 2019.) – Zašto je relevantan za kibernetičku sigurnost?



MRevS 315 (izmijenjen 2019.) daje revizoru okvir za razumijevanje IT okruženja i rizika koji proizlaze iz korištenja IT-a.

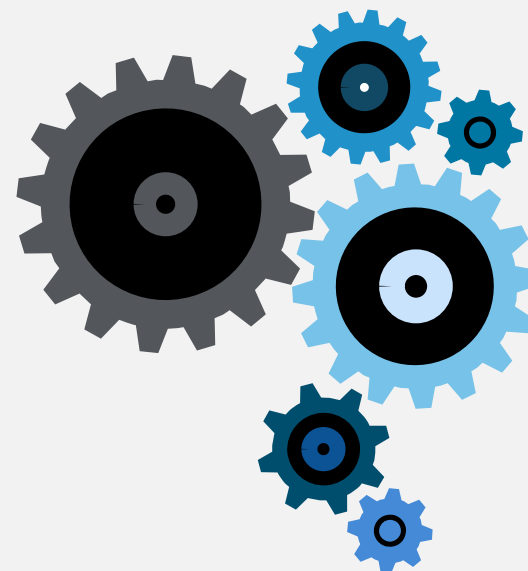
Što revizor treba razumjeti o IT okruženju?

Prema MRevS 315 (izmijenjen 2019,) fokus je na:



Input – Proces - Output

Koji dijelovi IT okruženja podržavaju financijski relevantne procese?



Rizici koji proizlaze iz korištenja IT-a

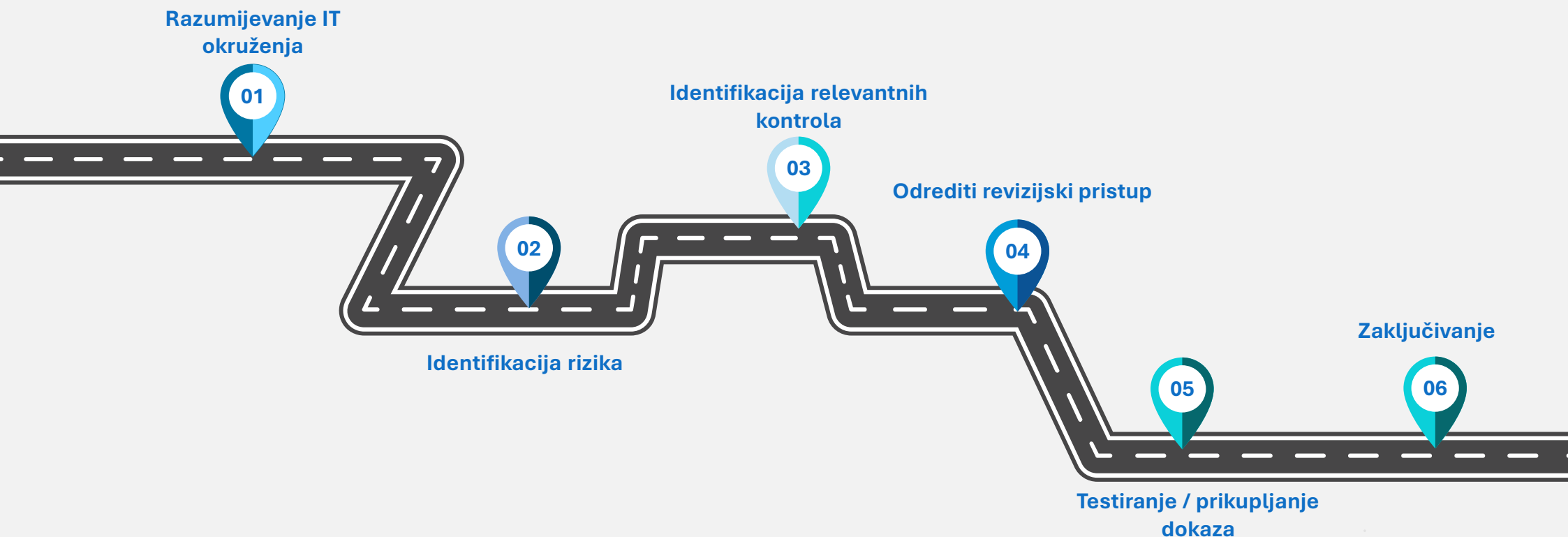


IT rizik	Kibernetički aspekt	Mogući utjecaj
Neovlašteni pristup	Krađa / kompromitacija vjerodajnica	Neovlaštene transakcije
Neovlaštene izmjene	Kompromitacija korisničkog računa	Neovlaštena izmjena podataka
Zlonamjerni softver / ransomware	Kibernetički napad	Nedostupnost sustava
Ranjivost sustava	Iskorištavanje ranjivosti	Kompromitacija sustava
IT kvar / neispravnost	Gubitak dostupnosti	Prekid poslovanja

GITC kao odgovor na IT rizike

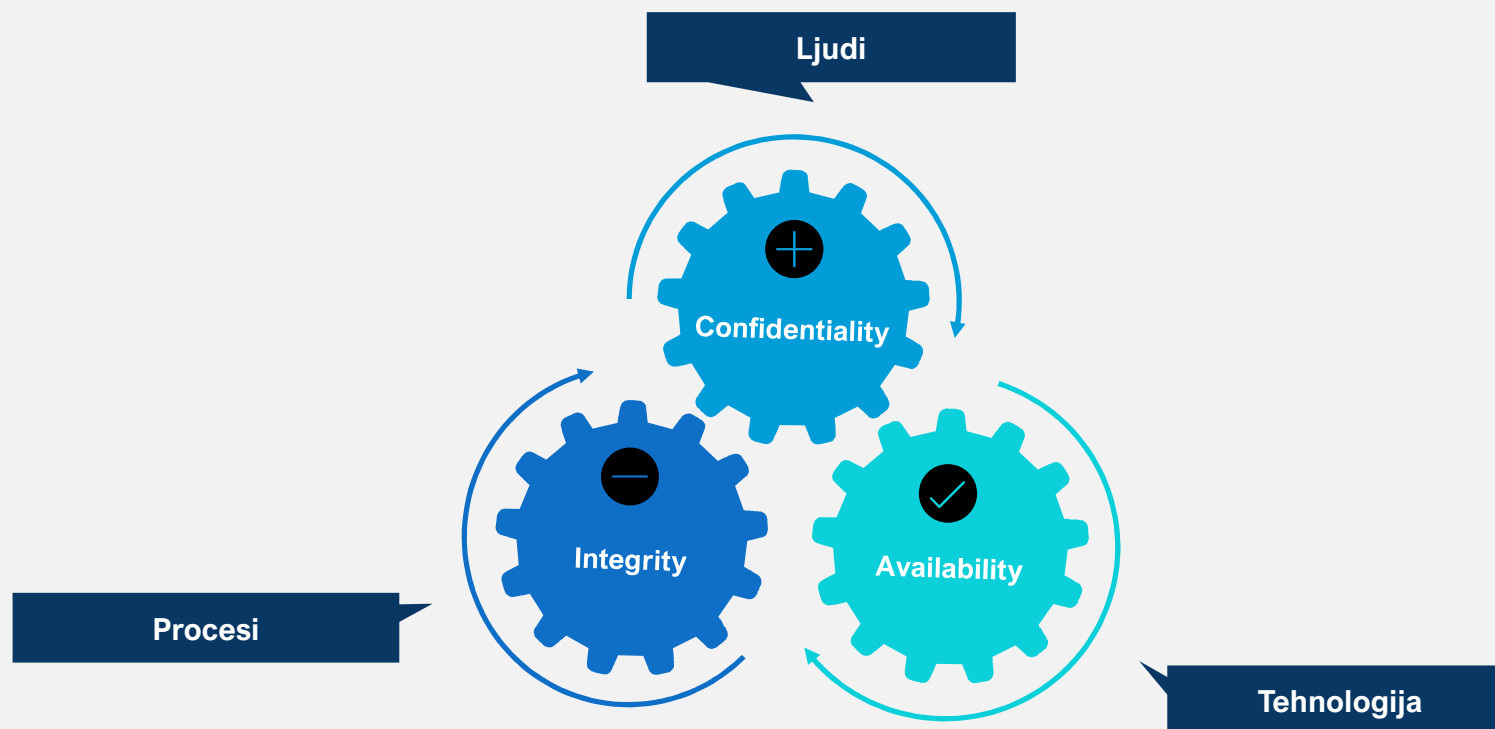


MRevS 315 (izmijenjen 2019.) – Od procjene do revizorskog postupka

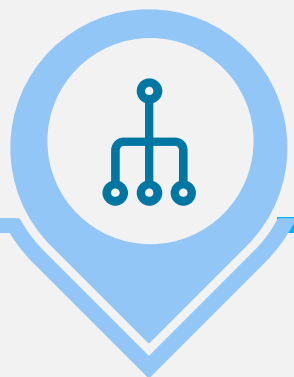


Informacijska sigurnost – ključne kontrole i područja provedbe

Informacijska sigurnost kao temelj kibernetičke sigurnost



Ključna područja kibernetičke sigurnosti



IDENTIFY

- Procjena kibernetičkih rizika
- Upravljanje imovinom
- Identifikacija prijetnji



PROTECT

- IAM / MFA
- Privilegiran pristup
- Upravljanje ranjivostima i zakrpama
- Sigurna konfiguracija



DETECT

- Upravljanje zapisima
- Siguran nadzor
- SIEM
- Detekcija prijetnji



RESPOND

- Upravljanje incidentima
- Odgovor na incidente
- Eskalacija i komunikacija



RECOVER

- Backup
- Oporavak nakon katastrofe
- Kontinuitet poslovanja



Kako revizor provjerava kontrole kibernetičke sigurnosti?



Primjer: Privilegirani pristup

Rizik

Kompromitirani administratorski račun omogućuje napadaču potpun pristup sustavu.

Kontrole

- Višefaktorska autentifikacija
- Načelo najmanjih ovlasti
- Kontrola odobravanja
- Periodična provjera pristupa
- Kontinuirano praćenje i nadzor

Revizorski dokazi

- Evidencija privilegiranih računa
- Dokazi o odobrenju pristupa
- Dokazi o periodičnoj provjeri pristupa
- Zapisi o autentifikaciji
- Zapisi o aktivnostima korisnika

Red flags

- ▶ Dijeljeni administratorski računi
- ▶ Neaktivni korisnički računi
- ▶ Prekomjerne ovlasti
- ▶ Nije omogućena višefaktorska autentifikacija (MFA)
- ▶ Nema praćenja i nadzora aktivnosti

Primjer: Skeniranje ranjivosti



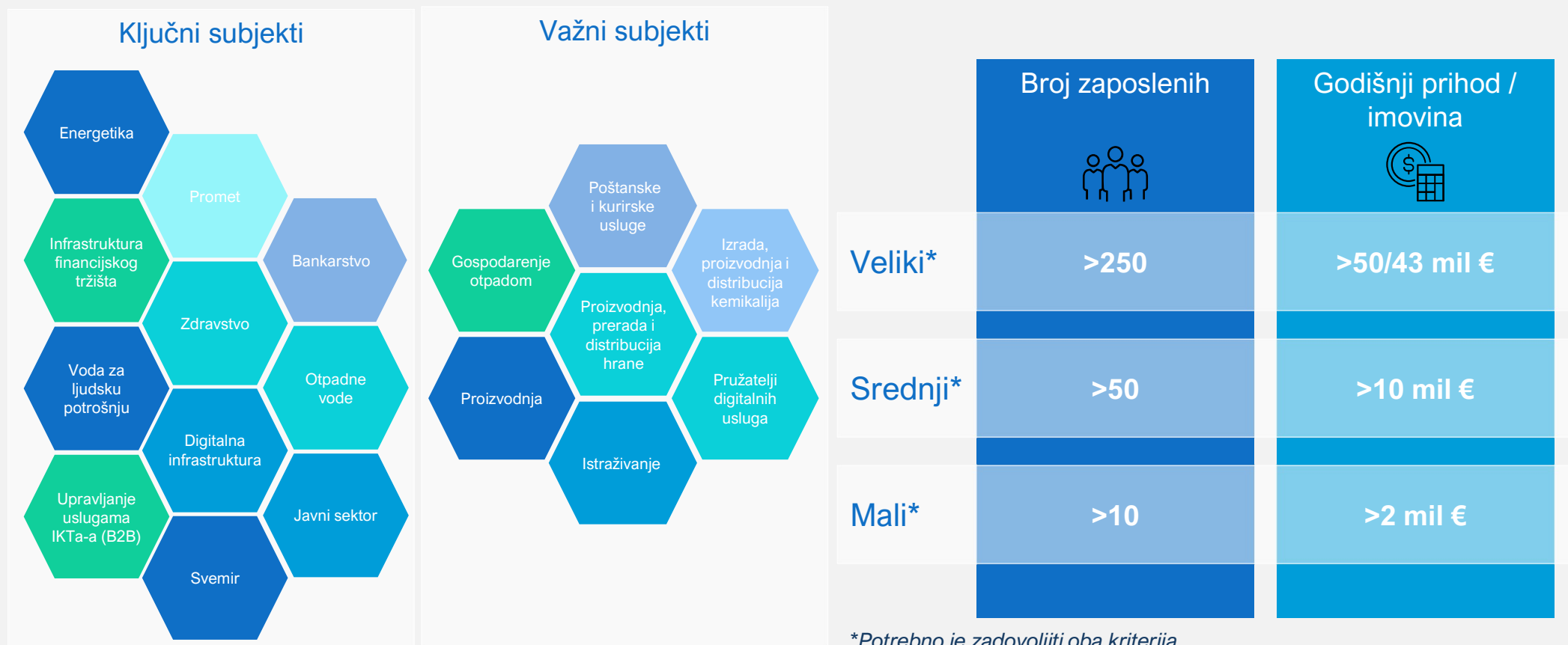
- Koliko često se provodi skeniranje ranjivosti?
- Kako se određuje razina kritičnosti ranjivosti?
- Postoji li definiran rok za otklanjanje ranjivosti (remediation SLA)?
- Kako se prate ranjivosti kojima je istekao rok za otklanjanje?
- Tko odobrava iznimke od zahtjeva za otklanjanje ranjivosti?
- Provjerava li se je li ranjivost doista otklonjena?



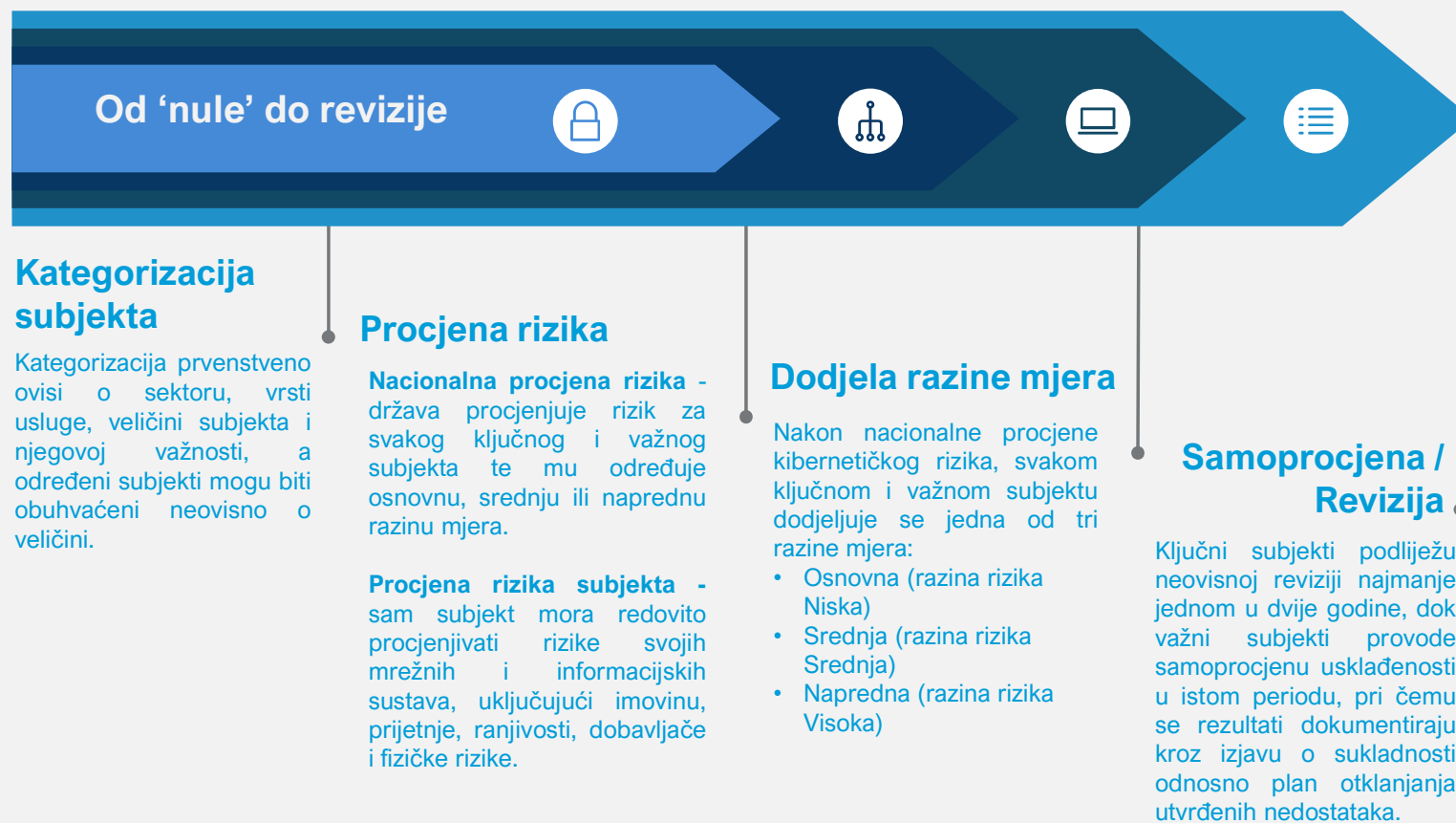
NIS2 - Regulatorni zahtjevi i revizorski pristup

Tko mora biti usklađen?

NIS2 se primjenjuje na javne i privatne subjekte iz obuhvaćenih sektora ovisno o njihovoj veličini ili posebnim kriterijima



Kako Uredba povezuje subjekte i obveze?



Nisu svi subjekti obvezni provoditi isti broj i istu složenost kontrola. Opseg zahtjeva ovisi o:

- *Kritičnosti subjekta*
- *Rezultatima procjene rizika*
- *Dodijeljenoj razini mjera*



Revizija kibernetičke sigurnosti



Tko?

Ključni subjekti

- Obvezna revizija

Važni subjekti

- Revizija na zahtjev nadležnog tijela



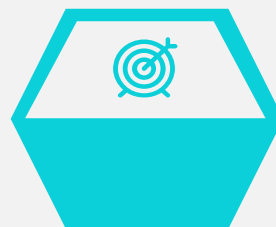
Koliko često?

Ključni subjekti

- Najmanje jednom u dvije godine

Važni subjekti

- Prema zahtjevu nadležnog tijela



Tko provodi?

Certificirani revizor kibernetičke sigurnosti – pružatelj upravljanih sigurnosnih usluga s odgovarajućim certifikatom.



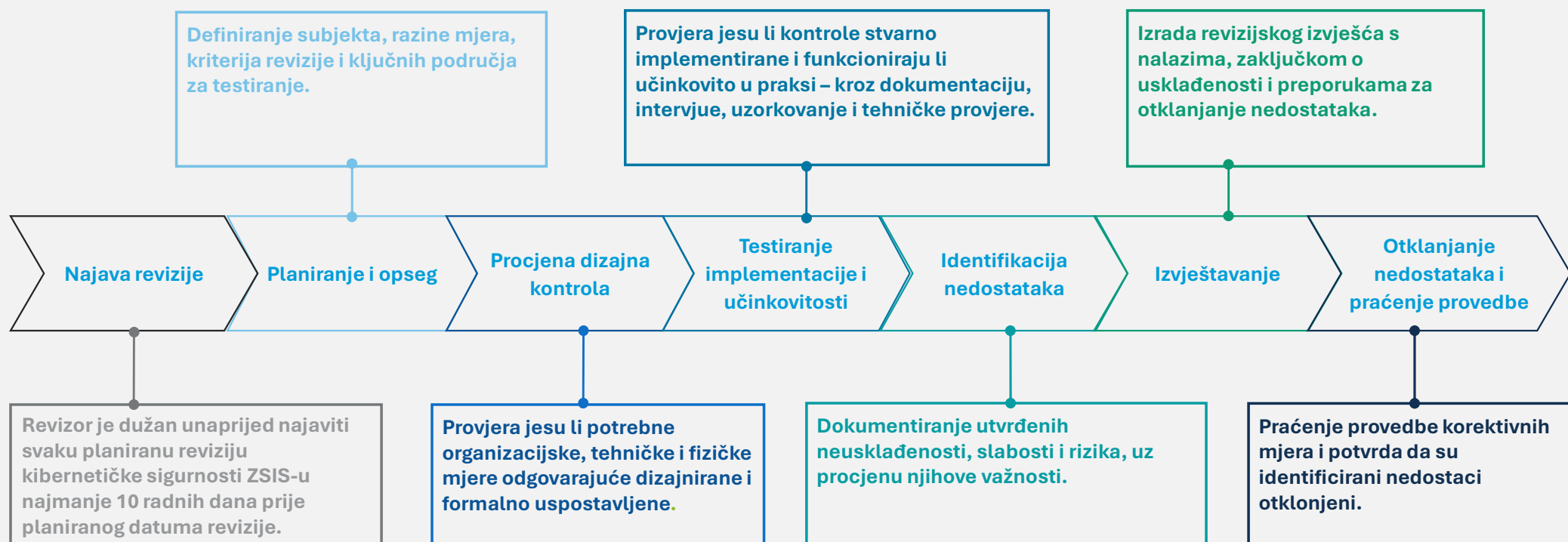
Što se postiže?

- Provjera usklađenosti
- identifikacija nedostataka
- Preporuke za poboljšanje
- Povećanje razine kibernetičke sigurnosti

Od regulatornog zahtjeva do dokaza usklađenosti – revizija potvrđuje da su zahtjevi Uredbe o kibernetičkoj sigurnosti ne samo formalno ispunjeni, već i učinkovito implementirani.



Revizijski proces



Ocjenjivanje kontrola kibernetičke sigurnosti

Ocjena	Dokumentacija	Implementacija
1 – Nedostatno	Dokumentacija ne postoji ili nije poznata provoditeljima	Proces se provodi ad hoc i bez praćenja
2 – Osnovno	Osnovna, nepotpuna ili neažurna dokumentacija	Proces je neformalan i provodi se sporadično
3 – Uspostavljeno	Formalno odobrena i ažurirana dokumentacija	Proces je strukturiran i redovito se provodi
4 – Napredno	Potpuna i ažurna dokumentacija, uz manje iznimke	Kontrola je potpuno implementirana, uz praćenje i izvještavanje
5 – Optimizirano	Kontinuirano poboljšavanje i minimalne iznimke	Napredno praćenje, kontinuirano poboljšavanje i minimalne iznimke

Ocjena kontrole određuje se kao aritmetička sredina ocjene dokumentacije kontrole i ocjene implementacije kontrole.



Svaka kontrola ima postavljen minimalni bodovni prag ocjene koji mora biti ispunjen kako bi se smatrala zadovoljenom.



Za prolazak podmjere nije dovoljno ispuniti samo pojedinačne bodovne pragove ocjena kontrola, već prosječna ocjena svih kontrola također mora zadovoljiti unaprijed definirani ukupni bodovni prag.



Zaključak

Što želimo dobiti iz provjere?



Od kibernetičkog rizika do revizorskog zaključka

- Identificiraj rizik
- Razumij kontrole
- Procjeni rizik
- Testiraj kontrole
- Prikupi dokaze
- Zaključči



Izvori i literatura:

- www.zsis.hr
- Interna dokumentacija Deloitte
- MRevS 315 (izmijenjen 2019.)



Hvala na pozornosti!



Marko Žalac



Deloitte



091 2370 091



mzalac@deloittece.com

